

Japanese Patent Laid-open No. 2003-283555 A

Publication date : October 3, 2003

Applicant : NIPPON TELEGRAPH AND TELEPHONE CORPORATION

Title : DISTRIBUTED DENIAL OF SERVICE ATTACK PREVENTING

5 METHOD AND GATE DEVICE, COMMUNICATION DEVICE, AND PROGRAM

[Scope of Claims for Patent]

[Claim 1]

A distributed denial of service attack preventing
10 method, wherein

in a network system including a network consisting of
a plurality of communication devices connected with each
other in a mesh, a computer and a LAN to be protected, and
a gate device which is inserted between the LAN and the
15 network,

the gate device, when a suspicious offensive traffic
is detected from an input communication traffic, executes
processing of calculating, based on a transmission band
limit value of the suspicious offensive traffic in the
20 corresponding gate device and the number of communication
devices in one-level-upstream of the corresponding gate
device, a transmission band limit value of the suspicious
offensive traffic to be notified to the upstream
communication devices, and transmitting a calculation
25 result to the upstream communication devices,

the communication device executes processing of
limiting a transmission band of the suspicious offensive
traffic to the transmission band limit value received from
the downstream gate device or communication device,
30 calculating, based on the received transmission band limit
value and the number of communication devices in one-level-
upstream of the corresponding communication device, a
transmission band limit value of the suspicious offensive

traffic to be notified to the upstream communication devices, and transmitting the calculation result to the upstream communication devices,

the communication device further executes recursive
5 processing of limiting the transmission band of a suspicious offensive packet, and transmitting the transmission band limit value of the suspicious offensive traffic until reaching the uppermost communication device serving as a sending end of the suspicious offensive packet,

10 the gate device executes processing of transmitting a query of an average input transmission band of the suspicious offensive traffic to the upstream communication device,

the upstream communication device executes processing
15 of receiving the query of the average input transmission band of the suspicious offensive traffic from the downstream gate device or communication device, and transmitting an average input transmission band value of the suspicious offensive traffic in the corresponding
20 communication device to the downstream gate device or communication device,

the gate device executes processing of calculating, based on a transmission band limit adjusted value of the suspicious offensive traffic in the corresponding gate
25 device and the average input transmission band value of the suspicious offensive traffic received from the upstream communication device, a transmission band limit adjusted value of the suspicious offensive traffic to be notified to the upstream communication device, and transmitting the
30 calculation result to the upstream communication device,

the communication device executes processing of limiting the transmission band of the suspicious offensive traffic to the transmission band limit adjusted value

received from the downstream gate device or communication device, and transmitting a query of the average input transmission band of the suspicious offensive traffic to the upstream communication device, and further executes
5 processing of calculating, based on the transmission band limit adjusted value received from the downstream communication device and the average input transmission band value of the suspicious offensive traffic received from the upstream communication device, a transmission band
10 limit adjusted value of the suspicious offensive traffic to be notified to the upstream communication device, and transmitting the calculation result to the upstream communication device, and

the communication device further executes recursive
15 processing of limiting the transmission band of the suspicious offensive packet to the transmission band limit adjusted value, and transmitting the transmission band limit adjusted value of the suspicious offensive traffic until reaching the uppermost communication device serving
20 as the sending end of the suspicious offensive packet.

[Brief Description of Drawings]

- [Fig. 1] A structural view of a network to which an embodiment of the present invention can be applied.
- 25 [Fig. 2] An example of setting conditions for detecting suspicious attacks according to the embodiment.
- [Fig. 3] An example of setting conditions for detecting illegal traffics according to the embodiment.
- [Fig. 4] A model of band control included in a gate device
30 2001 and communication devices 2002 to 2006 according to the embodiment.
- [Fig. 5] A classification algorism in a filter 2021 according to the embodiment.

[Fig. 6] A flowchart of an operation of the gate device 2001 according to the embodiment when a suspicious offensive packet is detected.

5 [Fig. 7] An example of calculation of a transmission band limit value in the configuration shown in Fig. of the embodiment.

[Fig. 8] A flowchart of an operation of the communication devices 2002 and 2003 according to the embodiment when receiving a transmission band limiting instruction.

10 [Fig. 9] A flowchart of an operation of the gate device 2001 and the communication devices 2002 to 2006 according to the embodiment when an illegal traffic is detected.

[Fig. 10] An example of calculation of a transmission band limit adjusted value in the configuration shown in Fig. of the embodiment.

15 [Fig. 11] A flowchart of an operation of adjusting the transmission band limit value performed by the gate device 2001 and the communication devices 2002 to 2006 according to the embodiment.

20

Fig. 1

2007, 2008

TERMINAL DEVICE

DDos ATTACKER

25

2009, 2010

TERMINAL DEVICE

LEGITIMATE USER

30 2002 to 2006 COMMUNICATION DEVICE (ROUTER)

NETWORK

2001 GATE DEVICE (GATEWAY)

2000
SERVER
DDos ATTACKED PERSON

5 Fig. 2
NUMBER
DETECTED ATTRIBUTE
DETECTED THRESHOLD
DETECTION INTERVAL
10 10 SECONDS
20 SECONDS

Fig. 3
NUMBER CONDITIONS OF ILLEGAL TRAFFIC
15 PACKETS OF T1 Kbps OR MORE ARE SUCCESSIVELY TRANSMITTED FOR
S1 SECOND OR LONGER.
ICMP/Echo Reply PACKETS OF T2 Kbps OR MORE ARE SUCCESSIVELY
TRANSMITTED FOR S2 SECONDS OR LONGER.
FRAGMENT PACKETS OF T3 Kbps OR MORE ARE SUCCESSIVELY
20 TRANSMITTED FOR S3 SECONDS OR LONGER.

Fig. 4
INPUT
2021 FILTER
25 2022 NORMAL CLASS
2023 NORMAL QUEUE
OUTPUT
2026 SUSPICIOUS CLASS
30 2027 SUSPICIOUS QUEUE
2024 ILLEGAL CLASS
2025 ILLEGAL QUEUE

Fig. 5

INPUT

S3003 DOES INPUT PACKET COINCIDE WITH ILLEGAL
SIGNATURE?

5 S3004 PUT IN ILLEGAL QUEUE

S3005 DOES INPUT PACKET COINCIDE WITH SUSPICIOUS
SIGNATURE?

S3006 PUT IN SUSPICIOUS QUEUE

S3007 PUT IN NORMAL QUEUE

10 OUTPUT

Fig. 6

START

S3011 DETECT SUSPICIOUS OFFENSIVE TRAFFIC

15 S3012 CREATE SUSPICIOUS SIGNATURE

S3013 REGISTER SUSPICIOUS SIGNATURE IN FILTER AND
CREATE SUSPICIOUS QUEUE

S3014 SEND TRANSMISSION BAND LIMITING INSTRUCTION TO
UPSTREAM COMMUNICATION DEVICE

20

Fig. 7

2007, 2008

TERMINAL DEVICE

DDos ATTACKER

25

2009, 2010

TERMINAL DEVICE

LEGITIMATE USER

30 2002 to 2006 COMMUNICATION DEVICE (ROUTER)

2001 GATE DEVICE (GATEWAY)

2000
SERVER
DDos ATTACKED PERSON

5 Fig. 8
START
S3021 RECEIVE TRANSMISSION BAND LIMITING INSTRUCTION
FROM DOWNSTREAM COMMUNICATION DEVICE
S3022 REGISTER SUSPICIOUS SIGNATURE IN FILTER AND
10 CREATE SUSPICIOUS QUEUE
S3033 SEND TRANSMISSION BAND LIMITING INSTRUCTION TO
UPSTREAM COMMUNICATION DEVICE

Fig. 9
15 START
S3031 DETECT ILLEGAL TRAFFIC
S3032 CREATE ILLEGAL SIGNATURE
S3033 REGISTER ILLEGAL SIGNATURE IN FILTER

20 Fig. 10
2007, 2008
TERMINAL DEVICE
DDos ATTACKER

25 2009, 2010
TERMINAL DEVICE
LEGITIMATE USER

OFFENSIVE PACKET

30
SUSPICIOUS OFFENSIVE PACKET

2002 to 2006 COMMUNICATION DEVICE (ROUTER)

2001 GATE DEVICE (GATEWAY)

2000

SERVER

5 DDos ATTACKED PERSON

Fig. 11

COMMUNICATION DEVICE (ROUTER)

START

10 S3061 RECEIVE QUERY OF AVERAGE INPUT TRANSMISSION BAND
FROM DOWNSTREAM COMMUNICATION DEVICE
S3062 TRANSMIT AVERAGE INPUT TRANSMISSION BAND VALUE TO
DOWNSTREAM COMMUNICATION DEVICE
S3063 RECEIVE TRANSMISSION BAND ADJUSTING INSTRUCTION
15 FROM DOWNSTREAM COMMUNICATION DEVICE
S3064 CHANGE TRANSMISSION BAND LIMIT VALUE TO
TRANSMISSION BAND LIMIT ADJUSTED VALUE
END

20 COMMUNICATION DEVICE (ROUTER)
START
S3051 RECEIVE QUERY OF AVERAGE INPUT TRANSMISSION BAND
FROM DOWNSTREAM COMMUNICATION DEVICE
S3052 TRANSMIT AVERAGE INPUT TRANSMISSION BAND VALUE TO
25 DOWNSTREAM COMMUNICATION DEVICE
S3053 RECEIVE TRANSMISSION BAND ADJUSTING INSTRUCTION
FROM DOWNSTREAM COMMUNICATION DEVICE
S3054 CHANGE TRANSMISSION BAND LIMIT VALUE TO
TRANSMISSION BAND LIMIT ADJUSTED VALUE
30 S3055 TRANSMIT QUERY OF AVERAGE INPUT TRANSMISSION BAND
TO ALL UPSTREAM COMMUNICATION DEVICES
S3056 RECEIVE AVERAGE INPUT TRANSMISSION BAND VALUE
FROM ALL UPSTREAM COMMUNICATION DEVICES

S3057 TRANSMIT TRANSMISSION BAND ADJUSTING INSTRUCTION
TO ALL UPSTREAM COMMUNICATION DEVICES
END

5 GATE DEVICE (GATEWAY)

START

S3041 TRANSMIT QUERY OF AVERAGE INPUT TRANSMISSION BAND
TO ALL UPSTREAM COMMUNICATION DEVICES

S3042 RECEIVE AVERAGE INPUT TRANSMISSION BAND VALUE

10 FROM ALL UPSTREAM COMMUNICATION DEVICES

S3043 SEND TRANSMISSION BAND ADJUSTING INSTRUCTION TO
ALL UPSTREAM COMMUNICATION DEVICES

S3044 DETECT TRIGGER

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-283555

(P2003-283555A)

(43) 公開日 平成15年10月3日(2003.10.3)

(51) IntCl. ⁷	識別記号	F I	テラワード(参考)
H 0 4 L 12/56	2 0 0	H 0 4 L 12/56	2 0 0 Z 5 K 0 3 0
12/46		12/46	E 5 K 0 3 3

審査請求 有 請求項の数13 O L (全 25 頁)

(21) 出願番号 特願2002-81905(P2002-81905)

(22) 出願日 平成14年3月22日(2002.3.22)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 柏 大

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 エリック・チェン

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

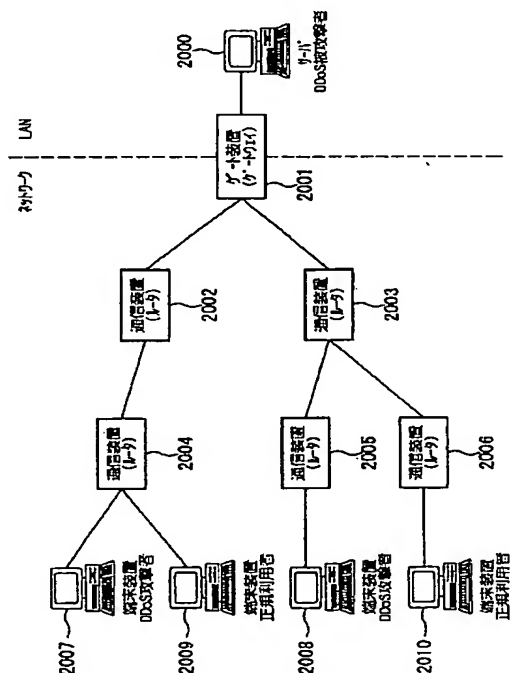
最終頁に続く

(54) 【発明の名称】 分散型サービス不能攻撃防止方法及びゲート装置、通信装置ならびにプログラム

(57) 【要約】

【課題】 正規利用者の通信トラフィックを確保しながら、分散型サービス不能攻撃（DDoS攻撃）の攻撃トラフィックの伝送帯域を制限することを可能とする。

【解決手段】 ゲート装置2001は、DDoS攻撃の攻撃容疑パケットを検出すると、上流の通信装置2002、2003に攻撃容疑パケットの伝送帯域制限値を通知する。上流の通信装置2002、2003は、攻撃容疑パケットの伝送帯域を受信した伝送帯域制限値に制限しながら、さらに上流の通信装置に伝送帯域制限値の通知を最上流まで繰り返し、各通信装置が攻撃容疑パケットの伝送帯域を制限する。一定時間経過後、ゲート装置2001は通信装置2002、2003から攻撃容疑パケットの平均入力伝送帯域値を受信し、この平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、各通信装置は再帰的に最上流の通信装置まで伝送帯域制限調整値を通知し、伝送帯域制限を調整する。



【特許請求の範囲】

【請求項 1】 複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよび LAN と、前記 LAN およびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、

前記ゲート装置は、

入力される通信トラヒックから攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の前記通信装置へ送信する処理を行い、

前記通信装置は、

前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限値に制限すると共に、前記受信した伝送帯域制限値と、当該通信装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、

前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、前記攻撃容疑パケットの伝送帯域の制限と、前記攻撃容疑トラヒックの伝送帯域制限値送信との処理を行い、

前記ゲート装置は、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理を行い、

前記上流の通信装置は、

前記下流のゲート装置または通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問合せを受信して、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置または通信装置へ送信する処理を行い、

前記ゲート装置は、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理を行い、

前記通信装置は、

前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限調整値に制限すると共に、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理と、前記下流の通信装置から受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調

整値を算出して前記上流の通信装置へ送信する処理とを行い、

前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、伝送帯域制限調整値に前記攻撃容疑パケットの伝送帯域の制限と共に、前記攻撃容疑トラヒックの伝送帯域制限調整値の送信との処理を行う、ことを特徴とする分散型サービス不能攻撃防止方法。

【請求項 2】 前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $S_s(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $S_s(d+1, i, k)$ とすると、

【数 1】

$$S_{s(d+1, i, k)} = \frac{1}{nu_{(d, i)}} S_{s(d, i)}$$

により算出されることを特徴とする請求項 1 に記載の分散型サービス不能攻撃防止方法。

【請求項 3】 前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $S_s'(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $S_s'(d+1, i, k)$ とすると、

【数 2】

$$S_{s'(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} S_{s'(d, i)}$$

により算出されることを特徴とする請求項 1 または請求

項 2 に記載の分散型サービス不能攻撃防止方法。

【請求項 4】 複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよび LAN との間に介挿されたゲート装置において、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出するトラヒック監視手段と、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記トラヒック監視手段によって検出された攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する帯域制限調整手段と、

を備えることを特徴とするゲート装置。

【請求項 5】 前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を Ss * 30

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} Ss'_{(d,i)}$$

により算出することを特徴とする請求項 4 に記載のゲート装置。

【請求項 6】 防御対象であるコンピュータおよび LAN を防御するゲート装置が接続されたネットワークのノードを構成する通信装置において、

下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限する帯域制御手段と、

前記受信した伝送帯域制限値と、当該通信装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、

前記下流のゲート装置あるいは通信装置から前記攻撃容

* (d, i) 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu_{(d, i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss_{(d+1, i, k)}$ とすると、

【数 3】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} Ss_{(d,i)}$$

により算出し、

前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'_{(d, i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu_{(d, i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B_{(d+1, i, k)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'_{(d+1, i, k)}$ とすると、

【数 4】

疑トラヒックの平均入力伝送帯域問い合わせを受信し、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置あるいは通信装置へ送信する帯域通知手段と、

前記下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限する帯域制御調整手段と、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、

前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値と前記受信した伝送帯域制限調

整値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して、前記上流の通信装置へ送信する帯域制限調整手段と、
を備えることを特徴とする通信装置。

【請求項 7】 前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss_{(d+1,i,k)}$ とすると、

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} Ss_{(d,i)}$$

により算出し、

前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B_{(d+1,i,k)}$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'_{(d+1,i,k)}$ とすると、

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} Ss'_{(d,i)}$$

により算出することを特徴とする請求項 6 に記載の通信装置。

【請求項 8】 複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよび LAN との間に介挿されたゲート装置上で実行されるコン

ピュータプログラムであって、

入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

【請求項 9】 防御対象であるコンピュータおよび LAN を防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムであって、

下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、

前記受信した伝送帯域制限値と、当該通信装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、

前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、

前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

【請求項 10】 前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出され、

前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さ d にある i で識別されるゲート装置または通信装置の 1 つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出されることを特徴とする請求項 8 または請求項 9 に記載の分散型サービス不能攻撃防止プログラム。

【請求項 11】 複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよび LAN との間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当

該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、

前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

10 当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【請求項 12】 防御対象であるコンピュータおよび LAN を防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、前記受信した伝送帯域制限値と、当該通信装置の 1 つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、

30 前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、

前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、

40 前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、

前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、

前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、

50 の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【請求項13】 前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

【数9】

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出され、

前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

【数10】

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出されることを特徴とする請求項11または請求項12に記載の分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに接続された機器をネットワーク経由での攻撃から防御するための、サービス不能攻撃の防止方法およびその装置ならびにそのコンピュータプログラムに関するものであ

る。

【0002】

【従来の技術】従来、TCP/IP (Transmission control protocol/internet protocol) などのネットワークプロトコルは、オープンとなっており、互いに信用されるグループで使われるように設計されている。このため、コンピュータのオペレーティングシステムでは、大量の通信トラフィック（データ等）を攻撃目標のサーバに送信することによって、ネットワークの伝送帯域やサーバの資源を消費して正当な利用者の利用を妨げようとするサービス不能攻撃（以下、「D o S (Denial of Service) 攻撃」と記す）を防ぐことは考慮されていない。このようなD o S攻撃に対する防御の方法は増えてきているが、複数箇所から同時に連携してD o S攻撃を行う「DD o S (Distributed Denial of Service) 攻撃」に対する防御の方法は未だ効果的な方法が開発されていない。

【0003】このDD o S攻撃に対する一防御の方法として、UUNET社のCenterTrackがある。

これは、インターネットのルータに診断機能を付加し、DD o S攻撃の送信元を追跡する技術である。

【0004】また、DD o S攻撃を検出したノードより攻撃元に近い上流ノードで攻撃トラフィックを制限するための技術としては、本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法（特願2001-274016）、AT&T社論文（R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson and S. Shenker: "Controlling high bandwidth aggregates in the network - extended version" (2001)）、IDIP (Intruder Detection and Isolation Protocol) (D. Schnackenberg, K. Djahandari and D. Sterne: "Infrastructure for intrusion detection and response", Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX), South Carolina (2000)) などがある。AT&T社論文及びIDIPは、攻撃検出イベントを攻撃経路の上流ノードへ伝達し、上流ノードで伝送帯域制限を行うための方式やプロトコルである。本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法は、ルータにインストールされている移動型パケットフィルタリングプログラムが、自らのプログラムの複製を作成し、その複製を上流ルータ移動させ、各上流ルータへ移動してきた移動型パケットフィルタリングプログラムは、それぞれDD o S攻撃者のホストからサーバに向けて送られているトラフィック全てを通過させないような技術である。

【0005】

【発明が解決しようとする課題】CenterTrackは、攻撃を受けた被害者が攻撃者を特定することを助ける技術ではあるが、実際に攻撃を受けているときにその攻撃を防御することはできない。加えて、複数箇所

に分散された分散型 D o S の攻撃元になっているコンピュータやそのコンピュータが接続されているネットワークの管理者に連絡をしないと、攻撃そのものを止めることはできないため、実質的には攻撃を止めるまでに何時間、あるいは何日もの時間がかかってしまうという問題点がある。

【0006】また、この出願の同発明者等が出願済みの分散型サービス不能攻撃の防止方法、AT&T論文及びIDIPにおいては、攻撃パケットと特定されたパケットを次ノードへ送出せず、全て破棄してしまう。よって、標的となるサーバのダウンやルータ装置の過負荷等によりサービスが停止する一次被害を防止することはできるが、正規利用者からのパケットを攻撃パケットと識別する方法がないため、誤って正規利用者からの正規パケットも攻撃パケットとして破棄してしまう可能性があり、正規利用者の利用性が低下するといった二次被害を引き起こしてしまうという問題がある。

【0007】本発明は、上記事情を考慮してなされたものであり、その目的は、正規利用者へのサービス性を低下させる被害を軽減しながらDDoS攻撃を防御できる、分散型サービス不能攻撃防止方法及び装置ならびにプログラムを提供することにある。

【0008】

【課題を解決するための手段】この発明は、上記の課題を解決すべくなされたもので、請求項1に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびLANと、前記LANおよびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、前記ゲート装置は、入力される通信トラヒックから攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の前記通信装置へ送信する処理を行い、前記通信装置は、前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限値に制限すると共に、前記受信した伝送帯域制限値と、当該通信装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、前記攻撃容疑パケットの伝送帯域の制限と、前記攻撃容疑トラヒックの伝送帯域制限値送信との処理を行い、前記ゲート装置は、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理を行い、前記上流の通信装置は、前記下流のゲート装置または通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問合せを受信して、当該通信装置における前記攻撃容疑ト

ラヒックの平均入力伝送帯域値を前記下流のゲート装置または通信装置へ送信する処理を行い、前記ゲート装置は、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理を行い、前記通信装置は、前記攻撃容疑トラヒックの伝送帯域を下流のゲート装置または通信装置から受信した前記伝送帯域制限調整値に制限すると共に、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信する処理と、前記下流の通信装置から受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する処理とを行い、前記攻撃容疑パケット送出元の最上流の前記通信装置に達するまで再帰的に、伝送帯域制限調整値に前記攻撃容疑パケットの伝送帯域の制限と共に、前記攻撃容疑トラヒックの伝送帯域制限調整値の送信との処理を行う、ことを特徴とする分散型サービス不能攻撃防止方法である。

【0009】請求項2に記載の発明は、請求項1に記載の分散型サービス不能攻撃防止方法であって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

【数11】

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出されることを特徴とする。

【0010】請求項3に記載の発明は、請求項1または請求項2に記載の分散型サービス不能攻撃防止方法であって、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さdにあるiで識別

されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

【数12】

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出されることを特徴とする。

【0011】請求項4に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびLANとの間に介挿されたゲート装置において、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出するトラヒック監視手段と、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記トラヒック監視手段によって検出された攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信する帯域制限調整手段と、を備えることを特徴とするゲート装置である。

【0012】請求項5に記載の発明は、請求項4に記載のゲート装置であって、前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号を

k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

【数13】

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

10 により算出し、前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

【数14】

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出することを特徴とする。

【0013】請求項6に記載の発明は、防御対象であるコンピュータおよびLANを防御するゲート装置が接続されたネットワークのノードを構成する通信装置において、下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限する帯域制御手段と、前記受信した伝送帯域制限値と、当該通信装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信する帯域制限指示手段と、前記下流のゲート装置あるいは通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域問い合わせを受信し、当該通信装置における前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置あるいは通信装置へ送信する帯域通知手段と、前記下流のゲート装置あるいは通信装置から攻撃容疑トラヒックの伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝

送帯域を前記伝送帯域制限調整値に制限する帯域制御調整手段と、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せ手段と、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信する伝送帯域値受信手段と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値と前記受信した伝送帯域制限調整値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して、前記上流の通信装置へ送信する帯域制限調整手段と、を備えることを特徴とする通信装置である。

【0014】請求項7に記載の発明は、請求項6に記載の通信装置であって、前記帯域制限指示手段は、前記伝送帯域制限値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出し、前記帯域制限調整手段は、前記伝送帯域調整値を、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

【数16】

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出することを特徴とする。

【0015】請求項8に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびLANとの間に介挿されたゲート装置上で実行されるコンピュータプログラムであって、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【0016】請求項9に記載の発明は、防御対象であるコンピュータおよびLANを防御するゲート装置が接続されるネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムであって、下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、前記受信した伝送帯域制限値と、当該通信装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、前記受信した伝送帯域制限調整値と、前記上

流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【0017】請求項10に記載の発明は、請求項8または請求項9に記載の分散型サービス不能攻撃防止プログラムであって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出され、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{j=1}^{nu_{(d, i)}} B_{(d+1, i, j)}} Ss'_{(d, i)}$$

により算出されることを特徴とする。

【0018】請求項11に記載の発明は、複数の通信装

置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびLANとの間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、入力される通信トラヒックをチェックし、分散型サービス不能攻撃の攻撃容疑トラヒックを検出した場合に、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限値と、当該ゲート装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して上流の通信装置へ送信するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、当該ゲート装置における前記攻撃容疑トラヒックの伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体である。

【0019】請求項12に記載の発明は、防御対象であるコンピュータおよびLANを防御するゲート装置が接続されたネットワークのノードを構成する通信装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、下流のゲート装置又は通信装置から攻撃容疑トラヒックの伝送帯域制限値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限値に制限するステップと、前記受信した伝送帯域制限値と、当該通信装置の1つ上流にある通信装置数とを基に、上流の前記通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限値を算出して、上流の通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる伝送帯域問合せを受信し、前記攻撃容疑トラヒックの平均入力伝送帯域値を前記下流のゲート装置又は通信装置へ送信するステップと、前記下流のゲート装置又は通信装置から伝送帯域制限調整値を受信し、前記攻撃容疑トラヒックの伝送帯域を前記伝送帯域制限調整値に制限するステップと、前記上流の通信装置へ前記攻撃容疑トラヒックの平均入力伝送帯域を問合せを送信するステップと、前記上流の通信装置から前記攻撃容疑トラヒックの平均入力伝送帯域値を受信するステップと、前記受信した伝送帯域制限調整値と、前記上流の通信装置から受信した前記攻撃容疑トラヒックの平均入力伝送帯域値とを基に、上流の通信装置へ通知する前記攻撃容疑トラヒックの伝送帯域制限調整値を算出して前記上流の通信装置へ送信するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プロ

グラムを記録することを特徴とする記録媒体である。

【0020】請求項13に記載の発明は、請求項11または請求項12に記載の分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体であって、前記伝送帯域制限値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss(d+1, i, k)$ とすると、

$$Ss_{(d+1, i, k)} = \frac{1}{nu_{(d, i)}} Ss_{(d, i)}$$

により算出され、前記伝送帯域制限調整値は、ゲート装置または通信装置がゲート装置から何ホップ目に存在するかを示す階層の深さをd、同一の深さdにおいてゲート装置または通信装置を識別する番号をi、深さdにあるiで識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu(d, i)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にある通信装置を識別するための番号をk、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置から通知された攻撃容疑トラヒックの平均入力伝送帯域値を $B(d+1, i, k)$ 、深さdにあるiで識別されるゲート装置または通信装置の1つ上流にあるkで識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値を $Ss'(d+1, i, k)$ とすると、

$$Ss'_{(d+1, i, k)} = \frac{B_{(d+1, i, k)}}{\sum_{l=1}^{nu_{(d, i)}} B_{(d+1, i, l)}} Ss'_{(d, i)}$$

により算出されることを特徴とする。

【0021】

【発明の実施の形態】以下図面を参照し、この発明の一実施の形態について説明する。図1は、同実施の形態を適用したネットワークの構成図である。この図において、2000はサーバ、2001はこの発明の一実施形

態によるゲート装置（ゲートウェイ）、2002～2006はこの発明の一実施形態による通信装置（ルータ）、2007～2010は端末装置である。DDoS攻撃の被攻撃者のサーバ2000が収容されているLAN（ローカルエリアネットワーク）は、ゲート装置2001によって外部のネットワークに接続されている。そして、ネットワークは通信装置2002、2003、2004、2005、2006を有している。DDoS攻撃者によって操作された端末装置2007、2008が、攻撃パケットを被攻撃者のサーバ2000に向かって送信すると、攻撃パケットが被攻撃者収容LANに集中して混雑が発生することにより、ゲート装置2001の資源を消費してしまい、DDoS攻撃者とは無関係な正規利用者の端末2009、2010からサーバ2000に接続できなくなるという現象が起こる。

【0022】ゲート装置2001は、予めサーバ2000を保有する利用者が設定した攻撃容疑検出条件を記憶している。図2に攻撃容疑検出条件の設定の例を示す。さらに、ゲート装置2001は、防御対象のサーバ2000及びサーバ2000が収容されているLANの所有者によって予め設定された伝送帯域制限値を記憶している。

【0023】図2における攻撃容疑検出条件は、検出属性、検出閾値及び検出間隔の組からなる3組のレコードで構成される。ここでは、番号はレコードを特定するために便宜上使用される。攻撃容疑検出条件は、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用され、3組のレコードの内のいずれかのレコードの条件にトラヒックが一致した場合、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。検出属性は、IPパケットの第3/4層属性種別とそれら属性値の組を指定するが、第3層属性であるIPの「Destination IP Address（宛先IPアドレス）」という属性種別は必ず指定される。図2において、番号1のレコードの検出属性は、「Destination IP Address（宛先IPアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、IPの上位層（第4層）のプロトコル種別を示す「Protocol（プロトコル）」が「TCP」であり（Protocol=TCP）、かつ、第4層プロトコルがどのアプリケーションの情報かを示す「Destination Port（宛先ポート番号）」が「80」である（Port=80）という属性種別とそれら属性値の組で指定される。番号2のレコード検出属性は、「Destination IP Address（宛先IPアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「UDP（User Datagram protocol）」である（Protocol=UDP）という属性種別とそれら属性値の組で指定される。また、番号3のレコード検出属性は、「Destination IP Address（宛先IPアドレス）」が「192.168.1.0/24」である属性種別とその属性

値で指定される。検出閾値は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を、検出間隔は同じく最低の連続時間を示している。

【0024】また、ゲート装置2001及び通信装置2002～2006は、攻撃容疑パケットのトラヒックを分析し、不正トラヒックを検出するための不正トラヒック検出条件を保有する。図3に不正トラヒック検出条件の設定の例を示す。ここでは、番号はレコードを特定するために便宜上使用される。不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。図3の番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上のパケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、第3層プロトコルであるICMP (Internet Control Message Protocol) 上のエコー応答 (Echo Reply) メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

【0025】ここで、ゲート装置2001及び通信装置2002～2006が備える帯域制御モデルを説明する。図4は本実施の形態におけるゲート装置2001及び通信装置2002～2006が備える帯域制御モデルを示す。帯域制御モデルは、入力パケットをクラス別に分類し、このクラスに従ってパケットの出力帯域制御を実現するためのモデルを示す。フィルタ2021は、入力されたパケットを正規クラス2022、容疑クラス2026、不正クラス2024の3つのクラスに分類する。なお、このフィルタ2021の分類アルゴリズムは後述する。正規クラス2022はデフォルトクラスであり、正規クラス2022に分類されたパケットは正規キュー2023につながれ、伝送帯域を制限せずに出力される。容疑クラス2026に分類されたパケットは、容疑パケットか否かを判断するための防御対象のサーバ2000及びサーバ2000が収容されているLAN毎に発生する容疑キュー2027につながれ、防御対象のサーバ2000及びサーバ2000が収容されているLANの所有者によって予め設定された伝送帯域制限値に出力伝送帯域が制限される。なお、容疑シグネチャの生成については後述する。サーバ2000を収容しているゲート装置2001の容疑キューの伝送帯域制限値は防御対象のサーバ2000及びサーバ2000が収容されて

いるLANの所有者によって予め設定された伝送帯域制限値を使用するが、上流の通信装置2002～2006では、下流の通信装置から受信した伝送帯域制限値を使用する。不正クラス2024に分類されたパケットは、不正キュー2025につながれ、サーバ所有者やネットワークのポリシーに関わらず、0または0に近い伝送帯域に制限される。

【0026】続いて、ゲート装置2001及び通信装置2002～2006が伝送帯域制限を実行するための、フィルタ2021の分類アルゴリズムについて説明する。ゲート装置2001及び通信装置2002～2006は、当該通信装置に入力される全ての通信パケットをこの分類アルゴリズムで分類する。図5はフィルタ2021における分類アルゴリズムを示す。まず、ステップS3003において、フィルタ2021は、入力されたパケットが不正シグネチャと合致するか判断する。不正シグネチャに合致した場合、パケットは不正クラス2024に分類される (ステップS3004)。不正シグネチャに合致しなかった場合は、ステップS3005に進み、パケットが容疑シグネチャであるか判断し、容疑シグネチャに合致すれば容疑クラス2026へ分類され (ステップS3006)、合致しない場合には正規クラス2022へ分類される (ステップS3007)。このようにして各クラスに分類されたパケットは、正規キューであれば伝送帯域を制限せずに出力され、容疑キュー及び不正キューであればそれぞれの伝送帯域制限値に従って伝送帯域が制限されて出力される。なお、容疑シグネチャ及び不正シグネチャの生成については後述する。

【0027】次に、DDoS攻撃に対する対策方式の処理手順を示す。まず、図6のゲート装置2001の攻撃容疑パケット検出時の動作を示すフローチャート、図8の通信装置2002、2003の伝送帯域制限指示受信時の動作を示すフローチャート及び図9のゲート装置2001及び通信装置2002～2006の不正トラヒック検出時の動作を示すフローチャートを用いてDDoS攻撃発生と同時に初期の伝送帯域制限を実施する処理手順を説明する。

【0028】図6のステップS3011において、ゲート装置2001は、攻撃容疑検出条件 (図2) に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、3組のレコードの内のいずれかのレコードに合致した場合、このトラヒックを攻撃容疑トラヒックとして検出する。すると、ステップS3012において、この検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を、容疑シグネチャとして生成する。容疑シグネチャは、攻撃容疑トラヒックの通信パケット、すなわち攻撃容疑パケットを識別するために用いられる。例えば、図2の設定例を用いて説明すると、番

号1のレコードの条件で検出されるパケットの容疑シグネチャは[dst=192.168.1.1/32, Protocol=TCP, Port=80]となる。

【0029】次いで、ステップS3013において、ゲート装置2001は、ステップS3012において生成した容疑シグネチャをフィルタ2021に登録する。次に、防御対象のサーバ2000及びサーバ2000が収容されているLANの所有者によって予め設定された伝送帯域制限値に攻撃容疑トラヒックの伝送帯域を制限するための容疑キュー2027を生成する。なお、同一防

御対象に関する容疑キューが既に生成済みの場合は、新たな容疑キューの生成は行わない。これにより、以後、図4に示す帯域制御モデルと図5に示すフィルタ2021の分類アルゴリズムに従って、容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限が実行される。

【0030】そして、ゲート装置2001は、ステップS3014において、容疑シグネチャと算出した攻撃容疑パケットの伝送帯域制限値とを含んだ伝送帯域制限指示を1つ上流にある通信装置2002、2003に送信する。ここで、伝送帯域制限値の算出方法を説明する。なお、本明細書においては、ゲート装置あるいは通信装置を識別するための添え字を持つ

【数21】

$$Ss_{(d+1,i,k)}, Ss_{(d,i)}, nu_{(d,i)}$$

などの変数を便宜上 $Ss_{(d+1,i,k)}$ 、 $Ss_{(d,i)}$ 、 $nu_{(d,i)}$ のように記述する。ネットワークにおいて、ゲート装置2001の存在する階層を初期値0として通信装置がゲート装置2001から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別される通信装置の攻撃容疑パケットの伝送帯域制限値を $Ss_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流（すなわち深さ $d+1$ ）にある通信装置数を $nu_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流（深さ $d+1$ ）にある通信装置を識別するための番号を k 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流（深さ $d+1$ ）にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限値を $Ss_{(d+1,i,k)}$ とする。このとき、伝送帯域制限値は、以下の式で算出される。

【数22】

$$Ss_{(d+1,i,k)} = \frac{1}{nu_{(d,i)}} Ss_{(d,i)}$$

よって、ゲート装置2001は、上記の式により、通信装置2002、2003に指示する伝送帯域制限値を算出する。これは、ゲート装置2001は、自身が持つ伝送帯域制限値を1つ上流の通信装置全てに均等に割り当

てることを示す。図7は図1の構成における伝送帯域制限値の算出の例を示す図である。この図において、ゲート装置2001は深さ $d=0$ であり、この深さ $d=0$ には1つの装置のみが存在するためゲート装置2001の i は1である。ゲート装置2001の伝送帯域制限値の初期値 $Ss_{(0,1)}$ は、攻撃容疑トラヒックを検出したときのレコードに対応した伝送帯域制限値である。ここでは例として、伝送帯域制限値が800kbp/sであったとする。そして、ゲート装置2001には2つの1つ上流の通信装置2002、2003が存在するため、1つ上流の通信装置数 $nu_{(0,1)}$ は2である。よって、ゲート装置2001には、1番目の1つ上流の通信装置2002の伝送帯域制限値 $Ss_{(1,1,1)}$ 及び2番目の1つ上流の通信装置2003の伝送帯域制限値 $Ss_{(1,1,2)}$ は、 $Ss_{(0,1)} = 800 \text{ kbp/s}$ を $nu_{(0,1)} = 2$ で除算した400kbp/sとなる。

【0031】次に、伝送帯域制限指示受信時の通信装置2002、2003の動作を説明する。図8のステップS3021において、通信装置2002、2003は、ゲート装置2001が送信した（ステップS3014）伝送帯域制限指示を受信する。次に、ステップS3022に進み、通信装置2002、2003は、受信した伝送帯域制限指示に含まれる容疑シグネチャをフィルタ2021に登録し、容疑シグネチャ及び攻撃容疑パケットの伝送帯域制限値に対応した容疑キュー2027を生成する。これにより、以後、図4に示す帯域制御モデルと図5に示すフィルタ2021の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限が実行される。

【0032】通信装置2002はステップS3023において、その上流にある通信装置2004に、通信装置2003はその上流にある通信装置2005及び2006に、受信した容疑シグネチャと、受信した伝送帯域制限値から算出した伝送帯域制限値とを含んだ伝送帯域制限指示を送信する。このときの算出方法は、ゲート装置2001のステップS3003と同様である。すなわち、通信装置2002、2003は、ゲート装置2001から受信した伝送帯域制限値を1つ上流の通信装置全てに均等に割り当てる。図7を用いて説明すると、通信装置2002、2003の深さ d は1であり、この深さ $d=1$ には2つの通信装置が存在し、その1番目の通信装置2002の i は1、2番目の通信装置2003の i は2である。通信装置2002の伝送帯域制限値 $Ss_{(1,1)}$ 及び通信装置2003の伝送帯域制限値 $Ss_{(1,2)}$ は、それぞれゲート装置2001から受信した伝送帯域制限値 $Ss_{(1,1,1)}$ 、 $Ss_{(1,1,2)}$ であり、すなわち400kbp/sである。そして、通信装置2002には1つの上流の通信装置2004が存在するため、1つ上流の通信装置数 $nu_{(1,1)}$ は1である。よって、通信装置2004の伝送帯域制限値 $Ss_{(2,1,1)}$ は、 $Ss_{(1,1)} = 40$

0 k b p s を $nu(1, 1) = 1$ で除算した 400 k b p s となる。一方、通信装置 2003 には 2 つの上流の通信装置 2005、2006 が存在するため 1 つ上流の通信装置数 $nu(1, 2)$ は 2 である。よって、通信装置 2005 の伝送帯域制限値 $S_s(2, 2, 1)$ 及び通信装置 2006 の伝送帯域制限値 $S_s(2, 2, 2)$ は、 $S_s(1, 2) = 400 \text{ k b p s}$ を $nu(1, 2) = 2$ で除算した 200 k b p s となる。

【0033】そして、通信装置 2004 は通信装置 2002 から、通信装置 2005、2006 は通信装置 2003 から伝送帯域制限指示を受信し、通信装置 2002、2003 におけるステップ S3021～S3022 と同様に動作する。通信装置 2004～2006 は、ルーチングテーブルなどにより上流に通信装置がないと判断できるため、ステップ S3023 は実行しない。

【0034】次に、ゲート装置 2001 及び通信装置 2002～2006 の不正トラヒック検出時の動作を説明する。図 9 のステップ S3031 において、ゲート装置 2001 及び通信装置 2002～2006 は、DDoS 攻撃者がパケットを送出しているネットワークを特定するため入力パケットを分析して、不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出する。すると、ゲート装置 2001 及び通信装置 2002～2006 は、ステップ S3032 において、この検出された不正トラヒック条件を満たすパケットの送信元 IP アドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとする。そして、ゲート装置 2001 及び通信装置 2002～2006 は、ステップ S3033 においてこの不正シグネチャをフィルタ 2021 に登録する。これにより、以後、図 4 に示す帯域制御モデルと図 5 に示すフィルタ 2021 の分類アルゴリズムに従って不正シグネチャで識別される攻撃パケットの伝送帯域はさらに制限される。すなわち、攻撃パケットは不正クラス 2024 に分類され、正規利用者からのパケットである正規パケットのみが攻撃容疑パケットとして容疑クラス 2026 に分類される。

【0035】以上説明した初期の伝送帯域制限を実施することにより、早期にネットワークの伝送帯域の溢れを防いだ後、攻撃容疑パケットの入力トラヒックに応じて、伝送帯域制限値の調整を実施する処理手順を説明する。図 10 は伝送帯域制限調整値の算出の例、図 11 はゲート装置 2001 及び通信装置 2002～2006 の伝送帯域制限値の調整の動作を示すフローチャートである。

【0036】図 10 において、図 7 に示す初期の伝送帯域制限後、端末装置 2007 から 2 M b p s、端末装置 2008 から 2 M b p s の攻撃パケットが送信されており、また、端末装置 2009 から 600 k b p s、端末装置 2010 からは 100 k b p s の攻撃容疑パケットが送信されている。

【0037】通信装置 2004 は、端末装置 2007 から入力される攻撃パケットを不正クラス 2024 に分類しており、当該通信装置 2004 に入力される全攻撃容疑トラヒックは端末装置 2009 から受信される 600 k b p s である。これは、初期の伝送帯域制限の手順で受信した伝送帯域制限値 $S_s(2, 1, 1) = 400 \text{ k b p s}$ より大きいため、下流の通信装置 2002 には、攻撃容疑トラヒックを 400 k b p s に帯域制限して出力している。通信装置 2002 は、上流の通信装置 2004 から入力される攻撃容疑トラヒックの伝送帯域が 400 k b p s であり、初期の伝送帯域制限の手順で受信した伝送帯域制限値 $S_s(1, 1, 1) = 400 \text{ k b p s}$ 以下であるため、下流のゲート装置 2001 には 400 k b p s の攻撃容疑トラヒックを出力している。

【0038】一方、通信装置 2005 は、端末装置 2008 から入力される攻撃パケットを不正クラス 2024 に分類しているため、下流の通信装置 2003 に出力している攻撃容疑トラヒックは 0 k b p s である。また、通信装置 2006 に入力される攻撃容疑トラヒックは、端末装置 2010 から受信される 100 k b p s である。これは初期の伝送帯域制限の手順で受信した伝送帯域制限値 $S_s(2, 2, 2) = 200 \text{ k b p s}$ 以下であるため、下流の通信装置 2003 には、そのまま 100 k b p s の攻撃容疑トラヒックを出力している。よって、通信装置 2003 は、上流の通信装置 2005、2006 から入力される攻撃容疑トラヒックの伝送帯域の合計が 100 k b p s と、初期の伝送帯域制限の手順で受信した伝送帯域制限値 $S_s(1, 1, 2) = 400 \text{ k b p s}$ 以下であるため、下流のゲート装置 2001 には 100 k b p s の攻撃容疑トラヒックを出力している。

【0039】図 11 のステップ S3041 において、ゲート装置 2001 は、初期伝送帯域制限実施から一定時間後、全上流の通信装置 2002、2003 に当該ゲート装置 2001 に入力される攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる。すると、ステップ S3051 において、通信装置 2002、2003 は、平均入力伝送帯域の問合せを受信する。そして、ステップ S3052 において、通信装置 2002、2003 は、自身の攻撃容疑トラヒックの平均入力伝送帯域値をゲート装置 2001 に通知する。

【0040】次に、ステップ S3042 においてゲート装置 2001 は、通信装置 2002、2003 から攻撃容疑トラヒックの平均入力伝送帯域値を受信する。すると、ステップ S3043 において、ゲート装置 2001 は、受信した平均入力伝送帯域値を基に算出した攻撃容疑パケットの伝送帯域制限調整値を含んだ伝送帯域制限調整指示を、全上流の通信装置 2002、2003 に送信する。ここで、伝送帯域制限値の算出方法を説明する。なお、本明細書においては、ゲート装置あるいは通信装置を識別するための添え字を持つ

【数23】

$$Ss'_{(d+1,i,k)}, B_{(d+1,i,k)}, T_{(d,i)}, Ss'_{(d,i)}$$

などの変数を便宜上 $Ss'_{(d+1,i,k)}$ 、 $B_{(d+1,i,k)}$ 、 $Ss'_{(d,i)}$ のように記述する。ネットワークにおいて、ゲート装置2001の存在する階層を初期値0として通信装置がゲート装置2001から何ホップ目に存在するかを示す階層の深さを d 、同一の深さ d においてゲート装置または通信装置を識別する番号を i 、深さ d にある i で識別されるゲート装置または通信装置の攻撃容疑パケットの伝送帯域調整値を $Ss'_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある通信装置数を $nu_{(d,i)}$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの平均入力伝送帯域値 $B_{(d+1,i,k)}$ 、深さ d にある i で識別されるゲート装置または通信装置の1つ上流にある k で識別される通信装置の攻撃容疑トラヒックの伝送帯域制限調整値 $Ss'_{(d+1,i,k)}$ とする。このとき、伝送帯域制限調整値は、以下の式で算出される。

【数24】

$$Ss'_{(d+1,i,k)} = \frac{B_{(d+1,i,k)}}{\sum_{l=1}^{nu_{(d,i)}} B_{(d+1,i,l)}} Ss'_{(d,i)}$$

よって、ゲート装置2001は、上記の式により、通信装置2002、2003に指示する伝送帯域制限調整値を算出する。これは、ゲート装置2001は、上流の通信装置の攻撃容疑トラヒックの平均入力伝送帯域の比率に従って、攻撃容疑トラヒックの伝送帯域値を調整することを示している。ただし、ゲート装置2001の伝送帯域制限調整値の初期値 $Ss'_{(0,1)}$ は伝送帯域制限値の初期値 $Ss_{(0,1)}$ と同じである。

【0041】図10の送帯域制限調整値の算出の例を用いて説明する。ゲート装置2001の1番目の1つ上流の通信装置2002からゲート装置2001に入力される攻撃容疑トラヒックの平均入力伝送帯域値 $B_{(1,1,1)}$ は400kbps、2番目の1つ上流の通信装置2003からゲート装置2001に入力される攻撃容疑トラヒックの平均入力伝送帯域値 $B_{(1,1,2)}$ は100kbpsである。よって、(数24)の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、 $B_{(1,1,1)} + B_{(1,1,2)} = 500\text{kbps}$ と算出される。また、伝送帯域制限調整値の初期値 $Ss'_{(0,1)} = Ss_{(0,1)}$ であるため、図7の例より、 $Ss'_{(0,1)}$ は800kbpsである。従って、1番目の1つ上流の通信装置2002の攻撃容疑トラヒックの伝送帯域制限調整値 $Ss'_{(1,1,1)}$ は、 $B_{(1,1,1)} = 400\text{kbps}$ を分母500kbpsで除算し、伝送帯域制限調整

値の初期値 $Ss'_{(0,1)} = 800\text{kbps}$ を乗算した640kbpsとなる。一方、2番目の1つ上流の通信装置2003の攻撃容疑トラヒックの伝送帯域制限調整値 $Ss'_{(1,1,2)}$ は、 $B_{(1,1,2)} = 100\text{kbps}$ を分母500kbpsで除算し、伝送帯域制限調整値の初期値 $Ss'_{(0,1)} = 800\text{kbps}$ を乗算した160kbpsとなる。

【0042】そして、図11のステップS3053において、通信装置2002、2003は、ゲート装置2001から伝送帯域制限調整指示を受信する。すると、ステップS3054に進み、通信装置2002、2003は、容疑キュー2027の伝送帯域制限値を受信した伝送帯域制限調整指示に含まれる伝送帯域制限調整値に変更する。これにより、以後、図4に示す帯域制御モデルと図5に示すフィルタ2021の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域は伝送帯域制限調整値に制限される。

【0043】次に、図11のステップ3055へ進み、通信装置2002はその上流にある通信装置2004に当該通信装置2002に入力される攻撃容疑トラヒックの平均入力伝送帯域を、通信装置2003はその上流にある通信装置2005及び2006に当該通信装置2003に入力される攻撃容疑トラヒックの平均入力伝送帯域を問い合わせる。通信装置2004～2006は、ステップS3061において、平均入力伝送帯域の問合せを受信する。するとステップS3062において、通信装置2004は、通信装置2002に、通信装置2005、2006は、通信装置2003に自身の攻撃容疑トラヒックの平均入力伝送帯域値を通知する。

【0044】続いて、ステップS3056において、通信装置2002、2003は、通信装置2004～2006から受信した平均入力伝送帯域値を受信する。すると、ステップS3057において、通信装置2002、2003は、受信した平均入力伝送帯域値を基に算出した攻撃容疑パケットの伝送帯域制限調整値を含んだ伝送帯域制限調整指示を、全上流の通信装置、すなわち、通信装置2002はその上流にある通信装置2004に、通信装置2003はその上流にある通信装置2005及び2006に送信する。このときの算出方法は、ゲート装置2001のステップS3043と同様である。

【0045】図10の送帯域制限調整の算出の例を用いて説明する。通信装置2002の1番目の1つ上流の通信装置2004の平均入力伝送帯域値 $B_{(2,1,1)}$ は400kbpsである。よって、(数24)の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、 $B_{(2,1,1)}$ と同値になる。また、通信装置2002の伝送帯域制限調整値の初期値 $Ss'_{(1,1)} = Ss'_{(1,1,1)}$ であるため、ステップS3043より、 $Ss'_{(1,1)}$ は640kbpsである。よって、通信装置2002の1番目の1つ上流の通信装置2

004の攻撃容疑トラヒックの伝送帯域制限調整値 $S_s'(2,1,1)$ は、 $B(2,1,1)=400\text{ kbps}$ を分母 400 kbps で除算し、伝送帯域制限調整値の初期値 $S_s'(1,1)=640\text{ kbps}$ を乗算した 640 kbps となる。

【0046】一方、通信装置2003の1番目の1つ上流の通信装置2005から通信装置2003に入力される攻撃容疑トラヒックの平均入力伝送帯域値 $B(2,2,1)$ は 0 kbps 、2番目の1つ上流の通信装置2006から通信装置2003に入力される攻撃容疑トラヒックの平均入力伝送帯域値 $B(2,2,2)$ は 100 kbps である。よって、(数24)の右辺の分母は、全上流の通信装置からの平均入力伝送帯域値の合計を示していることより、 $B(2,2,1)+B(2,2,2)=100\text{ kbps}$ と算出される。また、通信装置2003の伝送帯域制限調整値の初期値 $S_s'(1,2)=S_s'(1,1,2)$ であるため、ステップS3043より、 $S_s'(1,2)$ は 160 kbps である。従って、通信装置2005の攻撃容疑トラヒックの伝送帯域制限調整値 $S_s'(2,2,1)$ は、 $B(2,2,1)=0\text{ kbps}$ を分母 100 kbps で除算し、伝送帯域制限調整値の初期値 $S_s'(1,2)=160\text{ kbps}$ を乗算した 0 kbps となり、通信装置2006の攻撃容疑トラヒックの伝送帯域制限調整値 $S_s'(2,2,2)$ は、 $B(2,2,2)=100\text{ kbps}$ を分母 100 kbps で除算し、伝送帯域制限調整値の初期値 $S_s'(1,2)=160\text{ kbps}$ を乗算した 160 kbps となる。

【0047】そして、図11のステップ3063において、通信装置2004~2006は、通信装置2002、2003から伝送帯域制限調整指示を受信する。ステップS3064に進み、通信装置2004~2006は、容疑キュー2027の伝送帯域制限値を受信した伝送帯域制限指示に含まれる伝送帯域制限調整値に変更する。これにより、以後、図4に示す帯域制御モデルと図5に示すフィルタ2021の分類アルゴリズムに従って容疑シグネチャに合致する攻撃容疑パケットの伝送帯域は伝送帯域制限調整値に制限される。

【0048】一方、ステップS3044において、ゲート装置2001は、上記の伝送帯域制限調整から一定時間後、あるいは、受信する攻撃容疑パケットの伝送帯域が伝送帯域調整前と調整後である一定の割合変化した場合などのトリガを検出すると、再び伝送帯域調整を実行するステップS3041から伝送帯域制限調整値の調整を繰り返す。

【0049】ところで、以上説明した動作は、以下に記述するアクティブネットワーク上で実行される。

【0050】以下、図面を参照しこの発明の一実施形態を実行できるアクティブネットワークについて説明する。図12は、本実施形態が前提とするネットワークの構成である。図12に示すように、通信ネットワークは、複数の通信装置7001によって接続されている。

そして、通信装置7001には1台または複数台のユーザのコンピュータ7000を接続することができるようになっている。ユーザのコンピュータ7000相互間で通信データのやりとりを行う際には、送信元のユーザのコンピュータ7000が送信したパケットを通信ネットワーク上の各ノードに位置する通信装置7001が順次転送することにより、そのパケットを宛先のユーザのコンピュータ7000に届けるようにする。

【0051】次に、通信装置の構成について説明する。

図13は、通信装置7001の内部の構成を示すブロック図である。図13に示すように、通信装置7001には通信線7024a、7024b、7024c、7024dが接続されており、通信装置7001はこれらの通信線を介して隣接する他の通信装置との間でパケットを交換することができるようになっている。また、通信装置7001には、上記の各通信線7024a~7024dに対応したインタフェース部7023a~7023dと、パケットを転送する処理を行うための転送処理部7021と、パケットの転送の際の転送先の情報を記憶する転送先テーブル7022と、アクティブパケットに対する処理を行うためのアクティブネットワーク実行環境(ActiveNetwork Execution Environment)7010とが設けられている。なお、アクティブネットワーク実行環境7010は、内部に、アクティブコード(プログラム)を実行するためのコード実行部7011と、アクティブコードを記憶しておくためのコード記憶部7012とを備えている。なお、ここでアクティブコードとは、アクティブネットワークにおいてパケットに対する作用を行うコンピュータプログラムのコードである。

【0052】ここで、図13を参照しながら、この通信装置7001の動作例の概要を説明する。隣接する他の通信装置から通信線7024dを介してパケットが到着すると、インタフェース部7023dがそのパケットを受信し転送処理部7021に渡す。転送処理部7021は、渡されたパケットのヘッダ部分に格納されている送信元(source)アドレスと宛先(destination)アドレスを読み取り、さらにそれらのアドレスをキーとして転送先テーブル記憶部7022に記憶されている転送先テーブルを参照することによって、そのパケットにどう対処するかを決定する。

【0053】パケットへの対処は大きく2通りに分けられる。そのパケットに対してアクティブコードを適用する場合と、そのパケットをそのまま他の通信装置に転送する場合とである。転送先テーブルを参照した結果、そのパケットに対してアクティブコードを適用すべきものである場合には、転送処理部7021は、そのパケットをアクティブネットワーク実行環境7010に渡す。アクティブネットワーク実行環境7010においては、コード実行部7011がそのパケットを受け取り、そのパケットに対して適用すべきアクティブコードをコード記

憶部 7012 から読み出して実行する。なお、コード実行部 7011 は、アクティブコードを実行した結果、必要な場合には処理対象となったパケットを再び転送処理部 7021 に渡して他の通信装置に対して転送することもある。転送先テーブルを参照した結果、そのパケットにアクティブコードを適用せずそのまま他の転送装置に転送すべきものである場合には、転送処理部 7021 は、適切な転送先に対応したインタフェース部 (7023a や 7023b や 7023c など) に渡し、そのインタフェース部が通信線 (7024a や 7024b や 7024c など) を介してパケットを他の通信装置に転送する。

【0054】なお、ここでは通信線 7024d を介して他の通信装置からパケットが到着した場合を例として説明したが、他の通信線を介してパケットが到着した場合の処理も同様である。

【0055】次に、通信装置 7001 内の転送処理部 7021 がいかんしてパケットに対する処置 (アクティブコードを適用するか、単純に他の通信装置に転送するか) を決定するかを具体的に説明する。

【0056】本実施形態が基礎とするフレームワークでは、アクティブネットワーク実行環境はパケットの中において指定されている IP アドレスに基づいて起動される。ここで、全ての (グローバル) IP アドレスの集合を I と表わすものとする。また、送信元 IP アドレスが s であり宛先 IP アドレスが d であるようなパケットを (s, d) と表わすものとする。また、通信装置のアクティブネットワーク実行環境に格納されているすべてのアクティブコードはそれぞれ特定のユーザに属するものとし、ある特定のユーザの所有する IP アドレスの集合を O と表わすものとする。

【0057】本フレームワークでは、上記特定のユーザに属する個々のアクティブコードは、次に示す式による集合 A で表されるパケットであって、かつ当該アクティブネットワーク実行環境を備えた通信装置 (ノード) によって受信されたパケットに対してアクセスする権限を持つ。すなわち、

$$A = \{ (s, d) \in [(O \times I) \cup (I \times O)] \mid s \neq d \}$$

である。つまり、この式が意味するところの概略は、特定のユーザに属するアクティブコードは、当該ユーザが所有する全ての IP アドレスのいずれかを送信元または宛先のアドレスとするようなパケットに対してアクセス権を有するということである。

【0058】当該ユーザに属する n 個のアクティブコードがある通信装置 (ノード) に格納されているとき、 i 番目 ($1 \leq i \leq n$) のアクティブコードは、集合 C

(i) ($C(i) \subseteq A$) に属するパケットをキャプチャして処理することをアクティブネットワーク実行環境に対して予め要求しておく。つまり、当該ユーザに関し

て、アクティブネットワーク実行環境は、 $c(1) \cup c(2) \cup \dots \cup c(n)$ なる和集合の要素であるパケット (s, d) によって起動されるものであり、このようなパケットを「アクティブパケット」と呼ぶことができる。

【0059】図 14 は、図 13 に示した転送先テーブル記憶部 7022 に記憶されている転送先テーブルの一例を示す概略図である。上記のフレームワークを実現するために必要な情報は、このような転送先テーブルに格納することが可能である。

【0060】図 14 に示すように、転送先テーブルは、タイプ (Type) と宛先アドレス (Destination) と送信元アドレス (Source) と転送先 (Send to) の各項目を含んでいる。タイプの項目は、テーブルのエントリーのタイプを表わすものであり、「アクティブ (Active)」あるいは「通常 (Regular)」のいずれかの値をとる。宛先アドレスおよび送信元アドレスの項目は、転送対象のパケットの宛先 IP アドレスおよび送信元 IP アドレスにそれぞれ対応するものである。転送先の項目は、宛先アドレスと送信元アドレスの組み合わせがマッチしたパケットに関して、適用すべきアクティブコードの識別情報あるいは転送先の通信装置の IP アドレスを表わすものである。

【0061】タイプの値が「アクティブ」であるエントリーは、対象のパケットに適用するアクティブコードを指定するものであり、その転送先の項目にはアクティブコードを識別する情報が書かれている。タイプの値が「通常」であるエントリーは、対象のパケットの転送先の通信装置のアドレスを指定するものであり、その転送先の項目には転送先の通信装置の IP アドレスが書かれている。

【0062】図 14 に示す転送先テーブルの例において、第 1 のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「1. 2. 3. 4」であり、送信元アドレスが「Any (何でもよい)」であり、転送先が「アクティブコード A」となっている。これは、送信元アドレスがいかなるアドレスであっても、宛先アドレスが「1. 2. 3. 4」にマッチする場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコード A が実行されることを表わしている。また、第 2 のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「10. 50. 0. 0」であり、送信元アドレスが「11. 12. 13. 14」であり、転送先が「アクティブコード B」となっている。これは、宛先アドレスと送信元アドレスの両方がそれぞれ上記の値にマッチした場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコード B が実行されることを表わしている。また、第 3 のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「Any

(何でもよい)」であり、送信元アドレスが「157. 2. 3. 0」であり、転送先が「アクティブコードC」となっている。これは、宛先アドレスがいかなるアドレスであっても、送信元アドレスが「157. 2. 3. 0」にマッチする場合には該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードCが実行されることを表している。

【0063】なお、図14に示すように、転送先テーブルにおいては、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも上に存在している。そして、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも優先的に適用される。また、各エントリーは、通信装置へ到着したパケットのみに対して適用され、転送のために送出されるパケットに対しては適用されない。

【0064】以上説明した通信装置の構成をまとめる。図13に示したインタフェース部は、通信線毎に設けられており、当該通信線から到着するパケットを受信するとともに当該通信線に対してパケットを送出する処理を行う。また、転送先テーブル記憶部は、パケットの送信元アドレスまたは宛先アドレスまたはそれら両方のアドレスのパターンと、該パターンに対応するプログラム

(アクティブコード)の情報あるいは該パターンに対応する転送先アドレスの情報とが登録された転送先テーブルを記憶する。また、アクティブネットワーク実行環境は、前記プログラムを予め記憶しているとともに、このプログラムを実行する。また、転送処理部は、通信線から到着した受信パケットを前記インタフェース部から渡された際に、当該受信パケットの送信元アドレスまたは宛先アドレスに基づいて前記転送先テーブルを参照し、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応する転送先アドレスの情報が登録されていた場合には当該受信パケットを所定の転送先アドレスに向けて送出するように当該転送先アドレスに対応したインタフェース部に渡すとともに、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応するプログラムの情報が登録されていた場合には前記アクティブネットワーク実行環境部において当該プログラムを起動させるとともに当該プログラムに当該受信パケットを渡す。

【0065】次に、本実施形態におけるアクティブコードのセキュリティに関するモデルについて説明する。このセキュリティのモデルは、各々のアクティブコードが、アクティブコードの所有者に関わるパケットのみに対して作用することを保証するためのものである。そのために、このセキュリティのモデルは、公開鍵のインフラストラクチャの存在を前提として、それを利用することとする。

【0066】図15は、上記のセキュリティモデルとそ

のモデルにおける処理の手順を示す概略図である。図15において、符号7051はユーザAのユーザ端末装置、7061は認証局(Certification Authority)装置である。この認証局の機能は、公の機関によって提供されるものであっても良いし、あるいはISP(Internet Service Provider, インターネット接続サービス提供者)などによって提供されるものであっても良い。なお、図15に示す例では、ユーザ端末装置7051のIPアドレスは「1. 2. 3. 4」である。以下では、ユーザAが、アクティブコードAを通信装置7001に登録するための処理の手順を説明する。なお、以下において、ユーザAはアクティブコードAの開発者であっても良いが、その必然性はなく、他の開発者が開発したアクティブコードAをユーザAが入手し、それを通信装置7001に登録するものでも良い。

【0067】まず(1)で示すように、ユーザAのユーザ端末装置7051は、周知技術を用いて鍵のペアすなわち公開鍵と秘密鍵とを生成する。そして(2)で示すように、ユーザ端末装置7051は、上で生成された公開鍵を認証局装置7061に登録する。このとき、認証局装置7061は、ユーザ端末装置7051のIPアドレスを検証する。この検証が正しく行なわれると、公開鍵そのものと、ユーザAを識別するための情報と、ユーザ端末装置7051のIPアドレス「1. 2. 3. 4」が認証局装置7061に記憶される。

【0068】次に(3)で示すように、ユーザ端末装置7051は、上で生成された秘密鍵を用いてアクティブコードAに電子署名する処理を行う。そして(4)で示すように、ユーザ端末装置7051は、秘密鍵で署名されたアクティブコードAを通信装置7001に登録する処理を行う。

【0069】これを受けて通信装置7001は、(5)で示すように、アクティブコードAの登録を行ったユーザAの電子証明書を認証局装置7061から取得する。この電子証明書には、ユーザAを識別する情報と、そのIPアドレス「1. 2. 3. 4」と、上の(2)において登録された公開鍵そのものとが含まれている。そして(6)で示すように、通信装置7001は、上記の電子証明書から取り出したユーザAの公開鍵を用いて、上の(4)において登録されたアクティブコードAの電子署名を検証する。そして、これが正しく検証された場合には、通信装置7001は、アクティブコードAをアクティブネットワーク実行環境に導入する処理を行う。また、これに応じて、転送先テーブルに必要なエントリーが追加される。

【0070】なお、この(1)および(2)の処理が行われて一旦ユーザAの公開鍵が認証局装置7061に登録されると、ユーザ端末装置7051はその公開鍵に対応する秘密鍵を用いてアクティブモジュールをいくつでも通信装置7001に登録することも可能である。

【0071】つまり、通信装置 7001 は登録部（図示せず）を備えており、この登録部は、ユーザの端末装置から当該ユーザの秘密鍵で電子署名されたプログラムを受信し、当該ユーザの電子証明書を認証局装置から受信し、受信した電子証明書に含まれる当該ユーザの公開鍵を用いて前記電子署名されたプログラムの検証を行い、この検証が成功した場合には当該プログラムに対応するアドレスのパターンと当該プログラムの情報とを前記転送先テーブルに登録し、この検証が失敗した場合には当該プログラムの情報の前記転送先テーブルへの登録は行わないようにするものである。

【0072】なお、上で説明した通信装置へのアクティブコードの登録の手順が有効に機能するためには、次の 2 点が前提となる。第 1 の前提として、ユーザがどの通信装置（ノード）にアクティブコードを登録すれば良いかは事前にわかっている。あるいは、どの通信装置（ノード）にアクティブコードを登録すればよいか分かるためのディレクトリサービスが提供されている。第 2 の前提として、通信装置（ノード）は、目的の認証局の公開鍵を事前にオフラインで取得しているか、他の認証局から取得するか、あるいは他の何らかの手段で取得できる。

【0073】次に、矛盾の解消のための制御について説明する。ある通信装置（ノード）において、 n 個のアクティブコードが登録されており、 i 番目 ($1 \leq i \leq n$) と j 番目 ($1 \leq j \leq n$) のアクティブコードが、それぞれ集合 $C(i)$ ($C(i) \subseteq A$) と集合 $C(j)$ ($C(j) \subseteq A$) に属するパケットに対するものであると定義されているとき、集合 $(C(i) \cap C(j))$ が空集合ではないような i および j の組み合わせ（但し $i \neq j$ ）が存在する場合があります。つまり、あるパケットが i 番目のアクティブコードにも j 番目のアクティブコードにも適用されるような定義が行われている場合である。このような矛盾は、次の 2 通りのシナリオのいずれかによって解消することとする。

【0074】第 1 の矛盾の解消のシナリオは、パケット (s, d) に関して、

$$(s \in O(k) \wedge d \in O(l)) \wedge (k \neq l)$$

であるために、

$$(s, d) \in C(i) \cap C(j)$$

となる場合に関するものである。但し、 $O(k)$ および $O(l)$ は、それぞれユーザ k および l によって所有される IP アドレスの集合である。つまり、あるパケットに関して、送信元のユーザ用のアクティブコードと宛先のユーザ用のアクティブコードとの両方が通信装置に登録されており、そのような通信装置にこのパケット

(s, d) が到着した場合である。このような場合には、宛先のユーザのアクティブコードを優先的に適用することが望ましいと考えられる。

【0075】つまり、転送先テーブルに登録されている

パターンに、送信元アドレスのみが指定されていて宛先アドレスが何でもよいとされている第 1 のエントリーと、宛先アドレスのみが指定されていて送信元アドレスが何でもよいとされている第 2 のエントリーとが含まれており、受信パケットがこれら第 1 のエントリーと第 2 のエントリーとの両方にマッチしたときには、第 1 のエントリーよりも第 2 のエントリーを優先させて、当該第 2 のエントリーのパターンに対応するプログラムを起動するようにする。

10 【0076】このように、送信元のユーザのアクティブコードよりも宛先のユーザのアクティブコードを優先させることは、アクティブネットワークの機能を用いて DDoS（分散型 DDoS, Distributed Denial of Service）攻撃を防御するメカニズムを構築する場合に特に重要となる。そのようにすることによって、宛先のユーザつまり被攻撃者となり得る者のアクティブコードが、攻撃者となる可能性があるもののアクティブコードよりも優先されるためである。

20 【0077】第 2 の矛盾の解消のシナリオは、あるパケット (s, d) に関して適用されるべき 2 つ以上のアクティブコードが同一のユーザによって登録されている場合に関するものである。このような場合には、該当するアクティブコードのうちの最も古く登録されたものが、他のものよりも優先的に適用されるようにすることが望ましいと考えられる。こうすることにより、ユーザが新しいアクティブコードを登録しようとする際には、新しいアクティブコードを有効にするために事前に古いアクティブコードを削除することが保証されるからである。

30 【0078】次に、これまでに述べたようなアクティブネットワークのノードとして機能する通信装置のインプリメンテーションの例について説明する。図 16 は、Linux 上の Java（登録商標）仮想マシン（JVM）を用いてアクティブパケットの処理を行う通信装置を実現した場合の概略図である。

40 【0079】図 16 に示す例では、専用の IP スタックを処理（process）の一部として構築している。これによって、図 14 に示したような転送先テーブルを実現し、実行環境（アクティブネットワーク実行環境）からこの転送先テーブルにエントリーの追加や削除を行えるようにしている。また、これに伴い、カーネル（kernel）内の IP スタックは不要となるため、カーネルにおけるルーティングを不活性化している。そして、到着パケットのコピーがデータリンク部分から作成され、そのパケットがライブラリ `libcap` を通して Java（登録商標）仮想マシンで補足できるようにしている。

50 【0080】処理の一部として構築した専用の IP スタックは、アクティブパケット、つまり転送先テーブル上の所定の定義にマッチする IP アドレス（宛先 IP アドレス、送信元 IP アドレス、あるいはそれらの組み合わせ）を有するパケットは、実行環境上で起動されるアク

タイプコードに対して渡される。一方、アクティブパケット以外の通常のパケットは、カーネルにおける IP スタックと同様の方法で隣接する通信装置等へ向けた転送が行われる。アクティブパケットであれ通常パケットであれ、この通信装置から送出されるすべてのパケットは、ライブラリ `libnet` を通して送出される。こうすることにより、各々処理されたパケットのヘッダに記録された送信元アドレスは、元々の送信元アドレスのままの状態、ネットワークに送出されることとなる。

【0081】また、標準の Java（登録商標）の API（アプリケーションプログラムインタフェース）である「`java.security`」を用いることによってセキュリティモデルをインプリメンテーションすることが可能である。この標準 API は、セキュリティモデルを構築するために必要な機能のほとんどを提供している。また、証明書のための形式としては「X.509」証明書形式を用いることが可能であり、アクティブコードの所有者の IP アドレスを「X.509」の識別名（DN, distinguished name）の一部に含めることにより、本実施形態のセキュリティモデルを実現することができる。

【0082】なお、言うまでもなく、上記インプリメンテーションではコンピュータシステムを用いることによってアクティブネットワーク実行環境を備えた通信装置を構築している。そして、上述した一連の処理、すなわち到着パケットの複製の作成とその捕捉や、転送先テーブルを参照しながらのアクティブパケットおよび通常パケットの転送の処理や、アクティブネットワーク実行環境上でのアクティブコードの起動とその処理の実行や、処理されたパケットのネットワークへの送出などの各処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。

【0083】なお、上述した各コンピュータプログラムは、コンピュータ読取可能な記録媒体に記録されており、通信装置等に搭載された CPU（中央処理装置）がこの記録媒体からコンピュータプログラムを読み取って、攻撃防御あるいはサービスモジュール提供等のための各処理を実行する。また、「コンピュータ読み取り可能な記録媒体」とは、磁気ディスク、光磁気ディスク、ROM、CD-ROM 等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（RAM）のように、一定時間プログラムを保持しているものも含むものとする。

【0084】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝

送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されても良い。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

【0085】また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【0086】また、下流のゲート装置または通信装置から上流の通信装置へのデータの送信は、アクティブネットワークの使用に限定するものではなく、任意の通信プロトコルの使用が可能である。

【0087】また、ゲート装置及び通信装置はゲートウェイやルータに限られるものではなく、ブリッジ、イーサネット（登録商標）、インタフェース変換装置など、IP アドレスを持つ任意の通信ノードであっても良い。

【0088】以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0089】

【発明の効果】以上説明したように、DDoS 攻撃の被攻撃者の通信装置が DDoS 攻撃の攻撃の容疑トラヒックを検出すると、初期の伝送帯域制御により、その上流の各通信装置で攻撃容疑トラヒックの伝送帯域を制限することが可能になるため、早期にネットワークの輻輳を改善することが可能となり、DDoS 被攻撃者のサービスの停止を抑止することが可能になるとともに、正規利用者からの通信パケットの割合を増加させることが可能になる。

【0090】また、初期の伝送帯域制御による攻撃容疑パケットの帯域制限後は、各通信装置の攻撃容疑パケットの入力伝送帯域に応じて伝送帯域制限値が調整することが可能になるため、伝送帯域をネットワーク上の各通信装置に有効に分配することが可能となり、攻撃容疑パケットとして分類された正規パケットの伝送帯域を増加させ、正規ユーザのサービス性の低下を段階的に改善することが可能になる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態を適用できるネットワークの構成図である。

【図 2】 同実施の形態による攻撃容疑検出条件の設定の例である。

【図 3】 同実施の形態による不正トラヒック検出条件の設定の例である。

【図 4】 同実施の形態によるゲート装置 2001 及び通信装置 2002～2006 が備える帯域制御モデルで

ある。

【図5】 同実施の形態によるフィルタ2021における分類アルゴリズムである。

【図6】 同実施の形態によるゲート装置2001の攻撃容疑パケット検出時の動作を示すフローチャートである。

【図7】 同実施の形態による図1の構成における伝送帯域制限値の算出の例である。

【図8】 同実施の形態による通信装置2002、2003の伝送帯域制限指示受信時の動作を示すフローチャートである。

【図9】 同実施の形態によるゲート装置2001及び通信装置2002～2006の不正トラフィック検出時の動作を示すフローチャートである。

【図10】 同実施の形態による図1の構成における伝送帯域制限調整値の算出の例である。

【図11】 同実施の形態によるゲート装置2001及び通信装置2002～2006の伝送帯域制限値の調整の動作を示すフローチャートである。

【図12】 同実施の形態を実行できるアクティブネットワークが前提とするネットワークの構成である。

【図13】 同実施の形態を実行できるアクティブネットワークによる通信装置内部の構成を示すブロック図である。

【図14】 同実施の形態を実行できるアクティブネットワークによる転送先テーブル記憶部に記憶されている転送先テーブルの一例を示す概略図である。

【図15】 同実施の形態を実行できるアクティブネットワークによるセキュリティモデルとそのモデルにおけ

る処理の手順を示す概略図である。

【図16】 同実施の形態を実行できるアクティブネットワークの通信装置をLinux上のJava（登録商標）仮想マシン（JVM）を用いてアクティブパケットの処理を行うように実現した場合の概略図である。

【符号の説明】

2000…サーバ

2001…ゲート装置

2002～2006…通信装置

10 2007～2010…端末装置

2021…フィルタ

2022…正規クラス

2023…正規キュー

2024…不正クラス

2025…不正キュー

2026…容疑クラス

2027…容疑キュー

7000…ユーザのコンピュータ

7001…通信装置

20 7010…アクティブネットワーク実行環境

7011…コード実行部

7012…コード記憶部

7021…転送処理部

7022…転送先テーブル記憶部

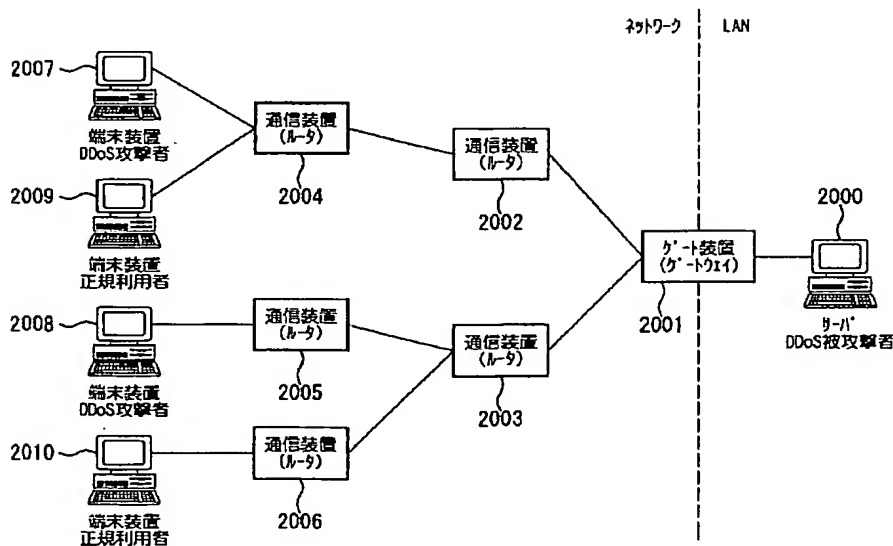
7023a、7023b…インタフェース部

7024a、7024b…通信線

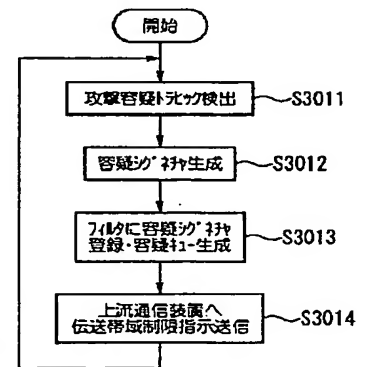
7051…ユーザ端末装置

7061…認証局装置

【図1】



【図6】



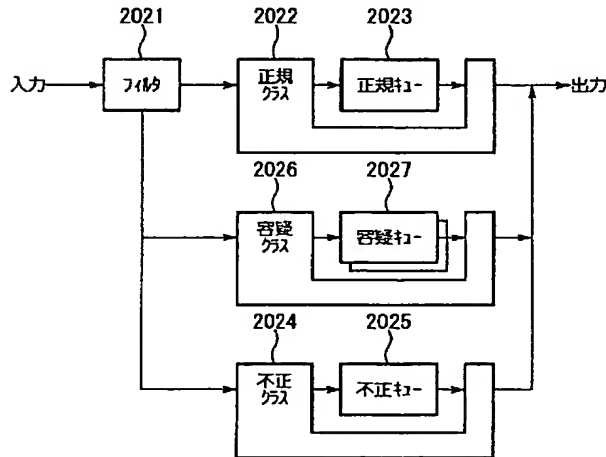
【図2】

番号	検出属性	検出閾値	検出間隔
1	[Dst=192.168.1.1/32,Protocol=TCP,Port=80]	500 kbps	10 秒
2	[Dst=192.168.1.2/32,Protocol=UDP]	300 kbps	10 秒
3	[Dst=192.168.1.0/24]	1 Mbps	20 秒

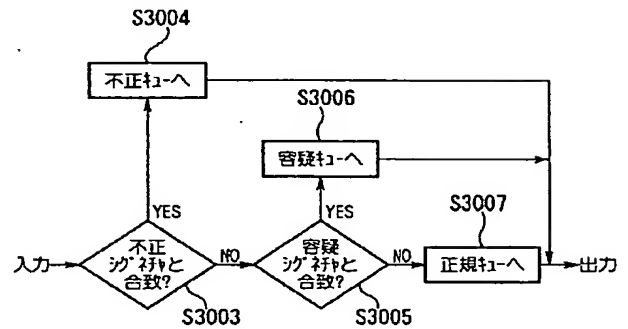
【図3】

番号	不正トラフィック条件
1	T1 Kbps 以上のパケットが S1 秒以上連続送信されている
2	T2 Kbps 以上の ICMP/Echo Reply パケットが S2 秒以上連続送信されている
3	T3 Kbps 以上のフラグメントパケットが S3 秒以上連続送信されている

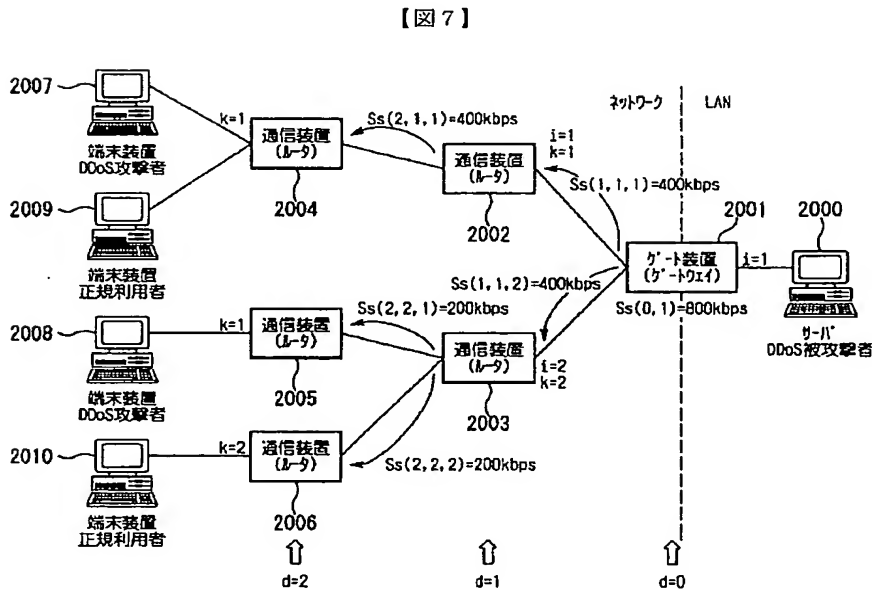
【図4】



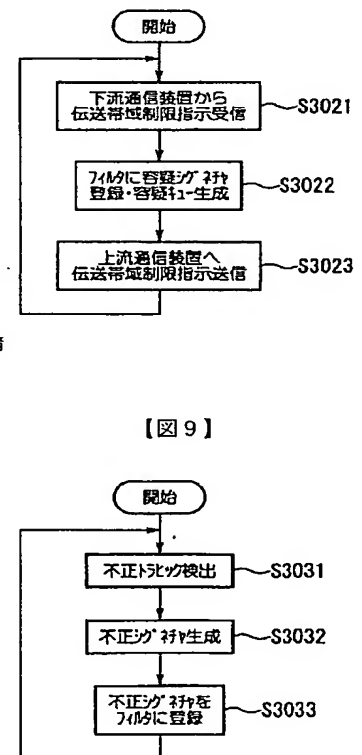
【図5】



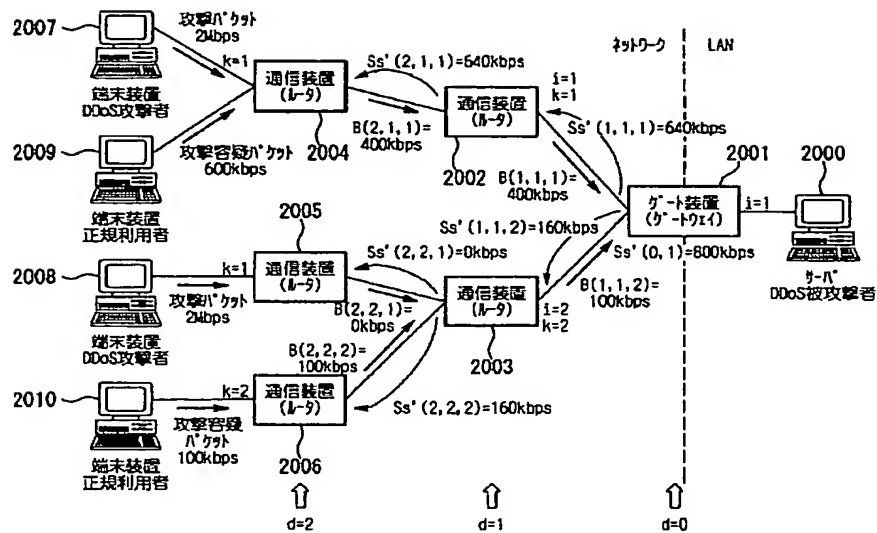
【図8】



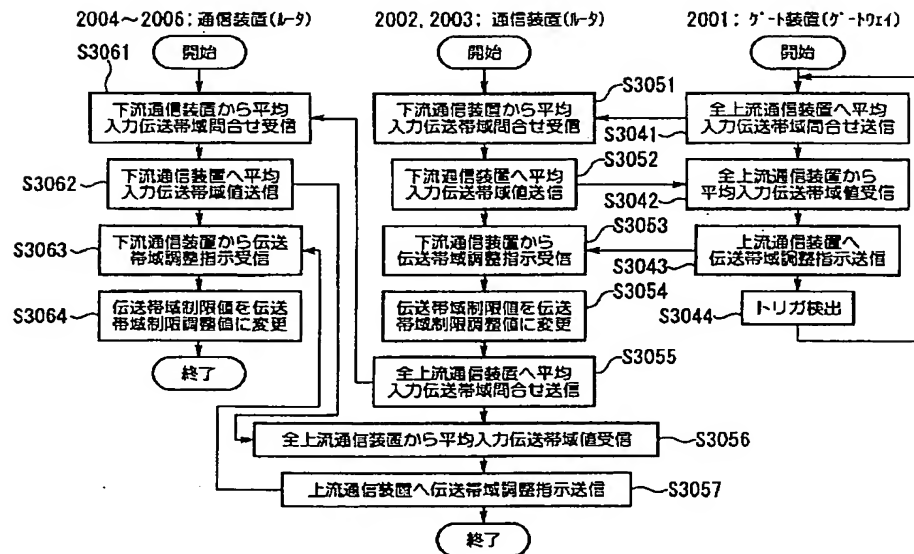
【図9】



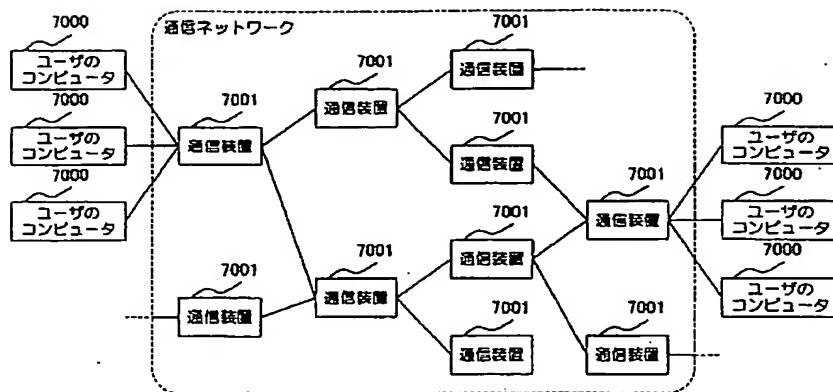
【図10】



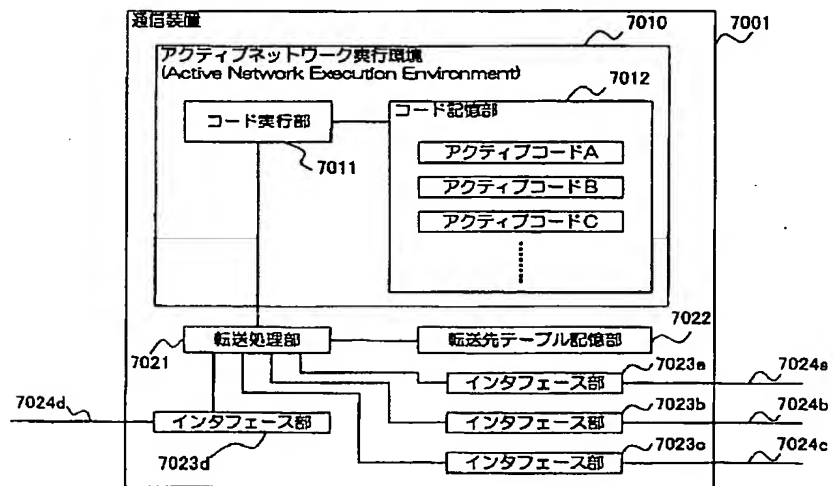
【図11】



【図12】



【図13】

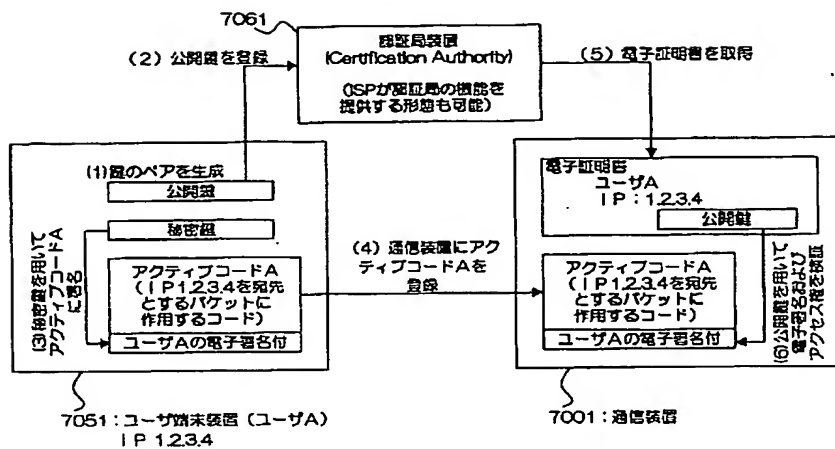


【図14】

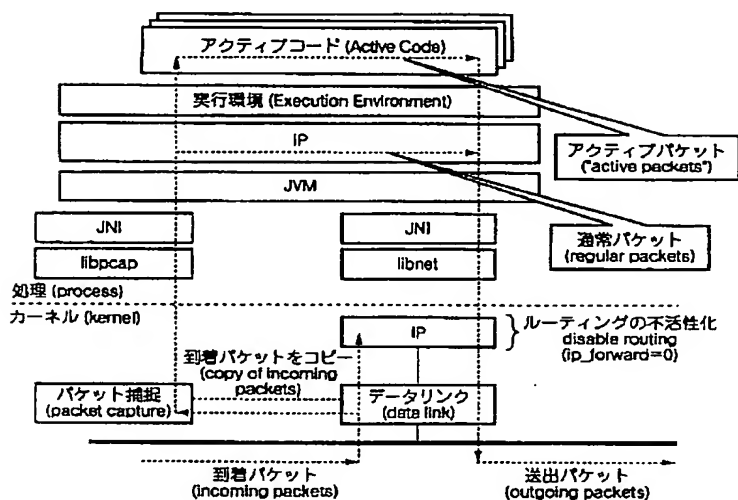
転送先テーブル

タイプ (Type)	宛先アドレス (Destination)	送信元アドレス (Source)	転送先 (Send to)
アクティブ (Active)	1.2.3.4	Any	アクティブコードA
アクティブ	10.50.0.0	11.12.13.14	アクティブコードB
アクティブ	Any	157.2.3.0	アクティブコードC
通常 (Regular)	1.2.0.0	N/A	29.15.20.1
通常	11.20.0.0	N/A	109.1.1.10
通常	199.1.1.0	N/A	120.0.0.1
...

【図15】



【図16】



フロントページの続き

(72) 発明者 富士 仁
東京都千代田区大手町二丁目 3 番 1 号 日
本電信電話株式会社内

F ターム (参考) 5K030 GA13 GA15 HA08 HB08 HB14
KA06 KX24 KX30 LC15 MD08
5K033 AA05 AA08 CB06 CB08 DA15
DB19 EA07